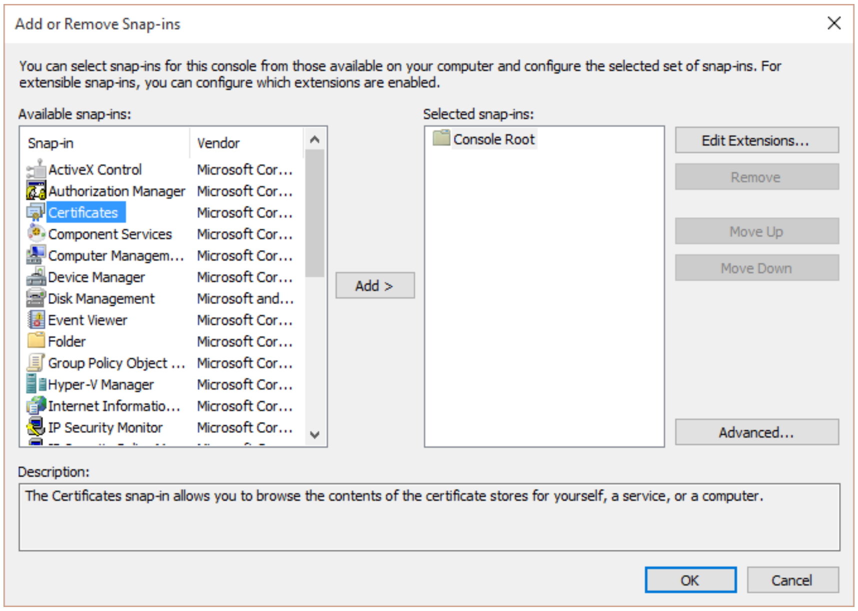
# Creating a Self-Signed Certificate

This document will walk through the steps of creating a self-signed security certificate. Note that self-signed certificates are useful for development purposes. In a production situation you will want to obtain a certificate from either your system administrator who uses Active Directory to create a certificate for use in your corporate domain, or use a third party certificate vendor such as Verisign.

In this document we will be using the Microsoft Management Console (MMC). The appearance of MMC will vary depending on what version of Windows it is running on, thus the screen shots in this document may not exactly match what is on your display. The steps though are the same regardless of the version of Windows.

1. Run the program MMC.EXE. (Note, the MMC application may appear different depending on the version of Windows you are running. The steps are basically the same regardless of the version of Windows you are using.)
2. Add the Certificate Snapin
   a. Select *File, Add/Remove Snap-in…* from the menu
   b. Select *Certificates* on the list of available snap-ins, then click *Add* to move it to the list of Selected snap-ins.



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

| Snap-in | Vendor |
|---|---|
| ActiveX Control | Microsoft Cor… |
| Authorization Manager | Microsoft Cor… |
| Certificates | Microsoft Cor… |
| Component Services | Microsoft Cor… |
| Computer Managem… | Microsoft Cor… |
| Device Manager | Microsoft Cor… |
| Disk Management | Microsoft and… |
| Event Viewer | Microsoft Cor… |
| Folder | Microsoft Cor… |
| Group Policy Object … | Microsoft Cor… |
| Hyper-V Manager | Microsoft Cor… |
| Internet Informatio… | Microsoft Cor… |
| IP Security Monitor | Microsoft Cor… |

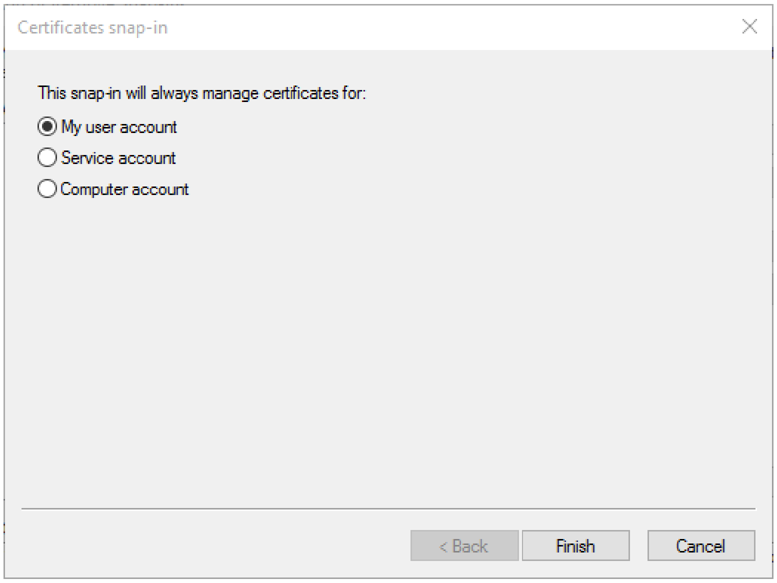
Selected snap-ins:

Console Root

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

   c. When you click the Add button, you will be prompted for which set of certificates to manage. Ensure *My user account* (the default) is selected and click *Finish*.



This snap-in will always manage certificates for:

● My user account
○ Service account
○ Computer account

d. Click *OK* to close the Add or Remove Snap-ins dialog.

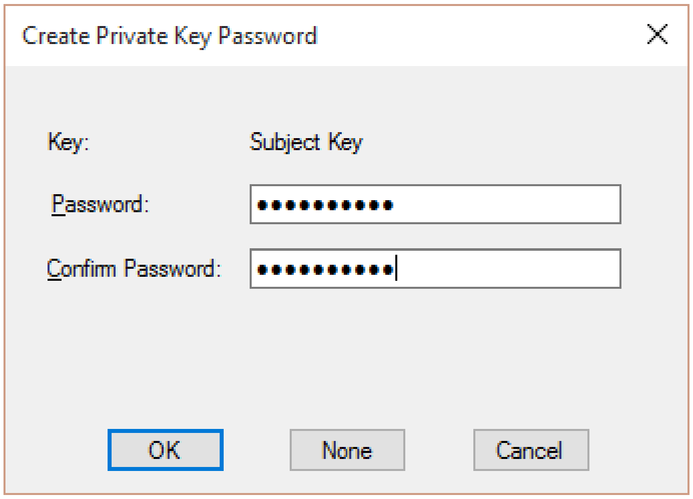
3. Next, you will want to open a Command Prompt window. You can search for it by typing CMD in the search window, the same way you searched for PowerShell. Make sure to right click on it, then select "*Run as administrator*".
4. You are going to run the makecert.exe program. It is included in either the Microsoft .Net Framework SDK or the Microsoft Windows Platform SDK. On the computer this document was developed on, Visual Studio 2013 with Update 5 is installed. There are multiple versions of MakeCert installed, the makecert utility used in this demo was be found in:

   C:\Program Files (x86)\Windows Kits\8.1\bin\x86

   If you are unsure of the location of use, just move to C:\Program Files (x86) in the Command Window, and type in `DIR MAKECERT.EXE /S`. This will look for makecert.exe in all of the subdirectories. You may find multiple copies, if so use the one with the most current date.
5. Once in the folder, enter the following command, all in one line (it wraps here due to document width limitations):

```
makecert -n "CN=PowerShell Local Certificate Root" -a sha1 -eku
1.3.6.1.5.5.7.3.3 -r -sv root.pvk root.cer -ss Root -sr localMachine
```

6. Upon hitting enter you will be prompted to enter a key. Either write it down, put it into a password safe such as LastPass, or use something you can remember.



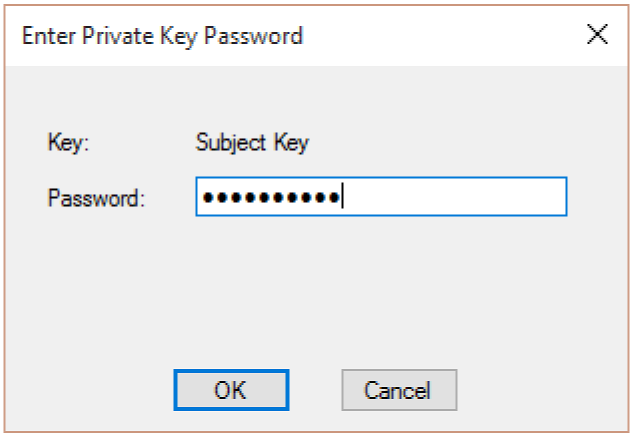
Create Private Key Password

Key: Subject Key

Password: ●●●●●●●●●●

Confirm Password: ●●●●●●●●●●

7. Click OK once you've entered the password. In the next screen you'll be prompted to enter your private key. This is the one you just entered when you created it, so just enter the same password again.

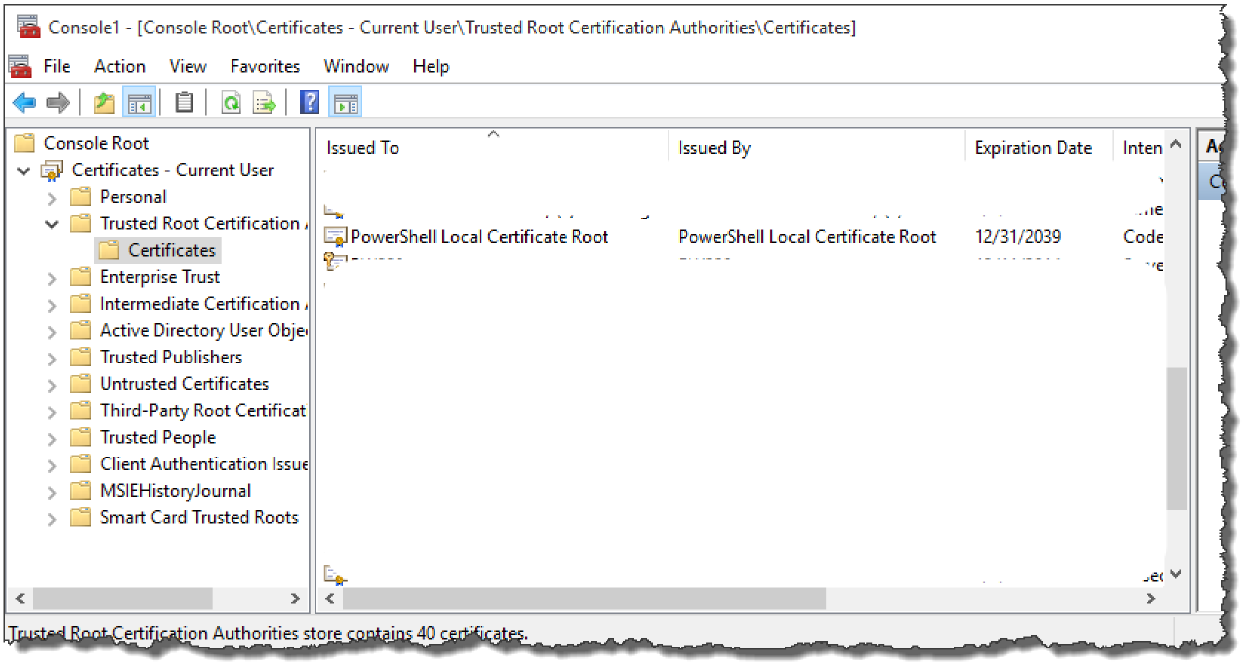


Enter Private Key Password

Key: Subject Key

Password: ●●●●●●●●●●

8. Return to MMC, and drill down to *Certificates – Current User, Trusted Root Certification Authorities, Certificates*. Scroll down and you should see the *PowerShell Local Certificate Root*. (Note for security reasons the other certificates in this image have been whited out).



Console1 - [Console Root\Certificates - Current User\Trusted Root Certification Authorities\Certificates]

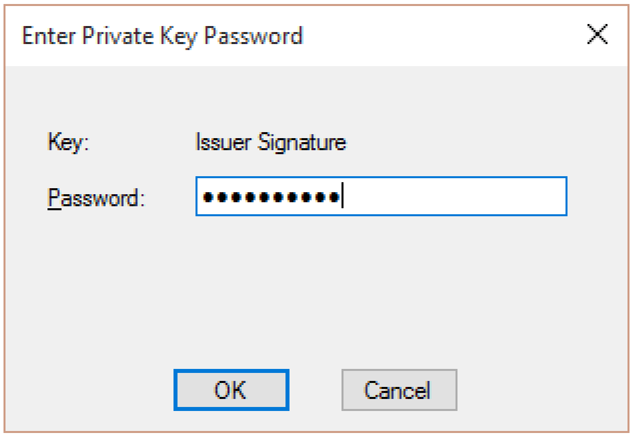
| Issued To | Issued By | Expiration Date | Inten |
|---|---|---|---|
| PowerShell Local Certificate Root | PowerShell Local Certificate Root | 12/31/2039 | Code |

Trusted Root Certification Authorities store contains 40 certificates.

9. Return to the command window and run the following command (again all on one line):

```
makecert -pe -n "CN=PowerShell User" -ss MY -a sha1 -eku
1.3.6.1.5.5.7.3.3 -iv root.pvk -ic root.cer
```

10. You will be prompted to enter your password. Enter and click OK.

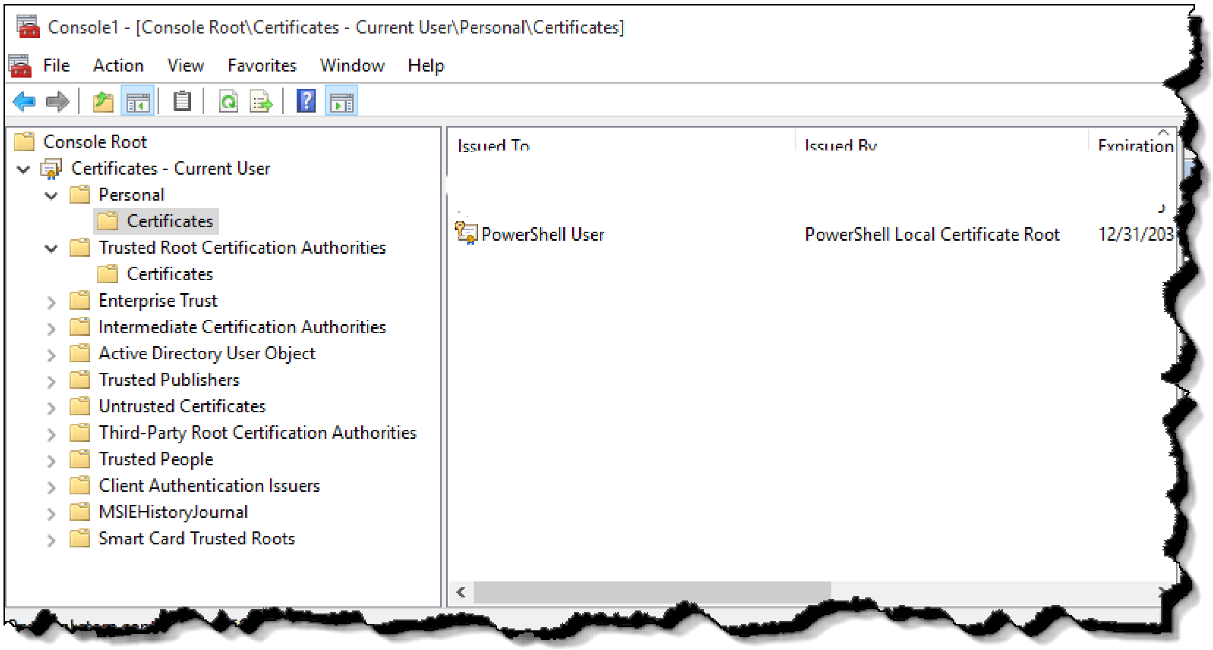


Enter Private Key Password

Key: Issuer Signature

Password: ●●●●●●●●●●●

11. Return to the MMC, and this time navigate to *Certificates – Current User, Personal, Certificates*. You should now see an entry for PowerShell User. (Again, other certificates have been whited out of this image for security reasons.)


Console1 - [Console Root\Certificates - Current User\Personal\Certificates]
File
Action
View
Favorites
Window
Help

- Console Root
  - Certificates - Current User
    - Personal
      - Certificates
    - Trusted Root Certification Authorities
      - Certificates
    - Enterprise Trust
    - Intermediate Certification Authorities
    - Active Directory User Object
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Authorities
    - Trusted People
    - Client Authentication Issuers
    - MSIEHistoryJournal
    - Smart Card Trusted Roots

| Issued To | Issued By | Expiration |
|---|---|---|
| PowerShell User | PowerShell Local Certificate Root | 12/31/203 |

12. Your certificate is now ready. Return to PowerShell to continue.